Uso de dispositivos móviles no corporativos

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. USO DE DISPOSITIVOS MÓVILES NO CORPORATIVOS (BYOD)

1.1. Antecedentes

El uso de dispositivos personales (portátiles, *smartphones*, *tablets*), propiedad del empleado, en el ámbito corporativo es lo que se conoce como *BYOD* (*Bring Your Own Device*) [8]. Se trata de una práctica muy frecuente, por lo tanto se debe prestar una especial atención para que su uso no comprometa la seguridad de la información de la empresa.

Existen ciertos riesgos que debemos conocer antes de permitir el uso de dispositivos personales en el ámbito corporativo:

- La exposición a redes inseguras en el ámbito personal. Este tipo de conexión podría tener como consecuencia que la información corporativa fuera accesible o pudiera ser interceptada por terceras personas no autorizadas.
- La instalación de aplicaciones que solicitan permisos para acceder a partes del dispositivo donde puede haberse almacenado información sensible, e incluso solicitar la activación de la geolocalización.
- La inexistencia de mecanismos de control de acceso a los dispositivos y la ausencia de medidas de seguridad en cuanto al almacenamiento de la información. Si alguien tuviera acceso a nuestro dispositivo no tendría ninguna dificultad a la hora de acceder o extraer información confidencial.
- La carencia de herramientas antivirus y de una normativa de actualizaciones adecuada. Actualizar las aplicaciones y disponer de un antivirus protegen al terminal de posibles ataques y accesos no autorizados.
- La opción (activada) de recordar y usar contraseñas de forma automatizada para acceder a redes, aplicaciones, sitios web, etc. Si alguien tuviera acceso al dispositivo no necesitaría disponer de las credenciales de usuario para acceder a la información.

Una vez establecida la política de seguridad relativa al uso seguro de los dispositivos personales para el trabajo, debe ponerse en conocimiento de los empleados y ser aceptada por los mismos antes de que utilicen sus dispositivos para acceder a aplicaciones o tratar con información de la empresa.

1.2. Objetivos

Establecer las normas que garanticen la seguridad de la información si se permite el uso de los dispositivos personales en el ámbito corporativo.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al **uso de dispositivos móviles no corporativos (BYOD).**

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
B	PRO	**Normas y procedimientos BYOD** Elaboras normas y procedimientos específicos si permites BYOD en tu empresa (usos permitidos, antivirus, actualización, configuraciones,…)	☐
B	PRO	**Prohibición de uso de dispositivos manipulados** Prohíbes el uso de dispositivos *rooteados* o a los que se ha realizado *jailbreak*.	☐
B	PRO	**Concienciación de los empleados** Involucras a los usuarios en la protección de sus propios dispositivos y de los datos que contienen o a los que pueden acceder.	☐
B	PRO	**Formación de los empleados** Proporcionas a tus empleados charlas o formación sobre cómo proteger sus dispositivos (contraseñas, actualizaciones, permisos, etc.).	☐
B	PRO	**Limitar el acceso a redes externas** Prohíbes el uso de redes inalámbricas externas no corporativas salvo 3G/4G.	☐
B	PRO/TEC	**Lista de aplicaciones no permitidas** Mantienes una lista de aplicaciones no permitidas y la difundes entre tus empleados.	☐
B	PRO/TEC	**Controlar el almacenamiento en la nube de datos corporativos** Supervisas el uso de aplicaciones de almacenamiento en la nube.	☐

NIVEL	ALCANCE	CONTROL	
B	PRO/TEC	**Proceso de borrado de la información** Aplicas una normativa de entrega/eliminación de la información de sus dispositivos cuando el empleado abandona la empresa.	☐
A	TEC	**Control de acceso a la red** Implementas un control de acceso (autenticación con contraseñas, doble factor, VPN…) a la red corporativa desde estos dispositivos.	☐
B	TEC	**Control de usuarios y dispositivos** Mantienes uno registro actualizado con usuarios, dispositivos y privilegios de acceso.	☐
B	TEC	**Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos** Instalas y configuras medidas para el almacenamiento seguro a la información (clasificación de información, cifrado de datos, etc.)	☐
B	TEC/PER	**Bloqueo programado** Configuras el bloqueo automático del dispositivo tras un periodo de inactividad.	☐
A	TEC/PER	**Extravío de dispositivos** Configuras medidas de seguridad para proteger la información corporativa en los dispositivos (localización, bloqueo de pantalla, borrado remoto de datos y seguimiento de las aplicaciones ejecutadas) en caso de extravío.	☐
B	PER	**Desconexión wifi y Bluethooth** Desactivas en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no son necesarios.	☐
B	PER	**Cumplimiento de la normativa** Conoces y aceptas la normativa corporativa vigente para el uso de tus dispositivos en actividades de la empresa.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Normas y procedimientos BYOD** [1]**.** El empresario elaborará normas y procedimientos específicos que regulen el uso de dispositivos BYOD (listado de dispositivos autorizados, en qué condiciones se permite su uso, cómo se accede a la información, configuraciones de seguridad necesarias para poder utilizarlos, etc.).
- **Prohibición de uso de dispositivos manipulados.** Se recomienda prohibir el uso de dispositivos *rooteados* o a los que se les ha hecho *jailbreak* ya que permiten la instalación de aplicaciones de repositorios no oficiales.
- **Concienciación de los empleados.** Los dispositivos como el teléfono móvil o el portátil son susceptibles de robo. Por ello es importante involucrar a los usuarios en la protección de sus propios dispositivos concienciándolos de la trascendencia de la protección del mismo y de los datos que contiene.
- **Formación de los empleados** [2]**.** Proporcionaremos a los empleados formación suficiente para un uso seguro de los dispositivos. Por ejemplo han de saber:
  - configurar los parámetros de seguridad de los dispositivos;
  - actualizar tanto el sistema operativo como las aplicaciones periódicamente (en especial el antivirus);
  - no instalar aplicaciones que exijan permisos que pongan en riesgo la información confidencial (acceso a la agenda, geolocalización, etc.);
  - bloquear los dispositivos con contraseña y activar el bloqueo automático tras un periodo corto de inactividad;
  - no desatender los dispositivos al viajar en transporte público.
- **Limitar el acceso a redes desconocidas** [3]**.** Los usuarios deben conocer que es preferible optar por la conexión de datos de su móvil 3G/4G/.. cuando las redes inalámbricas disponibles sean desconocidas. Estas redes wifi deben considerarse inseguras.
- **Lista de aplicaciones no recomendadas.** Estableceremos una lista de tipos de aplicaciones que no se podrán instalar en estos dispositivos por el peligro que suponen para la información corporativa. Estas aplicaciones pueden requerir para su instalación acceso a datos confidenciales de la organización (datos de la agenda, geolocalización del terminal, etc.).
- **Controlar el almacenamiento de datos corporativos.** Las aplicaciones personales en los dispositivos móviles para el tratamiento de datos en la nube no son tan seguras como las empresariales por lo que hay que prestar especial atención a este intercambio de archivos [4]. Se puede permitir la consulta de información en la nube pero se recomienda no actualizarla desde estos dispositivos personales.
- **Proceso de borrado de la información.** Estableceremos el proceso a seguir para entregar/eliminar la información en estos dispositivos cuando el empleado abandona la empresa.
- **Control de acceso a la red.** El acceso a la red corporativa a través de dispositivos personales debe estar integrado en el sistema de control de accesos (autenticación, doble factor,…). De esta forma el empleado debe acreditar su identidad antes de acceder a los servicios de la red corporativa. Para mayor seguridad la empresa puede proporcionar a sus empleados acceso mediante red privada virtual (VPN) que cifra las comunicaciones.

- **Control de usuarios y dispositivos.** Mantendremos un registro de usuarios y dispositivos que tienen acceso a los datos y aplicaciones de la empresa, detallando los privilegios de seguridad asignados para autorizar el acceso tanto a esos usuarios como a los dispositivos.
- **Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos.** Por ejemplo:
    - Implementaremos en los dispositivos mecanismos de cifrado de la documentación además de los de autenticación de usuarios.
    - Impediremos guardar de forma automática las credenciales de usuarios asociadas a las herramientas corporativas.
- **Bloqueo programado.** Configuraremos el dispositivo para que se bloquee automáticamente tras un periodo de inactividad.
- **Extravío de dispositivos.** Ante la posibilidad de pérdida o extravío de este tipo de dispositivos, estableceremos las siguientes medidas:
    - Localización mediante GPS, wifi o la información de la antena de telefonía con la que esté conectado el dispositivo. Una vez marcado como «perdido», el Smartphone empieza a enviar los datos de su ubicación de manera constante a una cuenta previamente configurada (correo, SMS, central de control...).
    - Tener siempre activado el bloqueo de pantalla del terminal. En caso contrario se bloqueará de manera remota.
    - Borrado remoto de datos: esta opción permite que los datos contenidos en el dispositivo se borren de manera remota, impidiendo su utilización por un usuario no legítimo.
    - Vigilar las aplicaciones que se ejecutan. El seguimiento de las llamadas efectuadas y las redes sociales accedidas entre otros, suelen ser datos suficientes para obtener nombres, apellidos y hasta direcciones de un posible delincuente.
- **Desconexión wifi y Bluethooth.** Se desactivará en el teléfono la búsqueda de redes wifi y de dispositivos vía Bluetooth cuando no sean necesarios.
- **Cumplimiento de la normativa.** Nos aseguraremos que los empleados conocen la normativa corporativa y se comprometen a cumplirla antes de la incorporación de sus dispositivos personales al entorno de trabajo.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Blog – Incorporación segura de dispositivos móviles a la empresa· https://www.incibe.es/protege-tu-empresa/blog/incorporacion-segura-dispositivos-moviles-empresa

[2]. Incibe – Protege tu empresa – Blog – Cinco consejos para la utilización segura de BYOD · https://www.incibe.es/protege-tu-empresa/blog/cinco-consejos-utilizacion-segura-byod

[3]. Incibe – Protege tu empresa – ¿Qué te interesa? – Protección en movilidad y conexiones inalámbricas · https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-movilidad-conexiones-inalambricas

[4]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en la nube https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[5]. Incibe – Protege tu empresa – Blog – Trabajando con dispositivos personales (BYOD) https://www.incibe.es/protege-tu-empresa/blog/trabajando-dispositivos-personales-byod-ciberseguridad-empresas

[6]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Almacenamiento en los equipos de trabajo https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[7]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Uso de wifis y redes externas https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[8]. Incibe – Protege tu empresa – Guías – Dispositivos móviles personales para uso profesional (BYOD): una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/dispositivos-moviles-personales-uso-profesional-byod-guia-aproximacion-el

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD